REMARKS

This Amendment is being filed in response to the outstanding Office Action, dated March 13, 2003 in which the Examiner rejected claims 1-6 and 8-24, all of the claims currently pending in the subject application. Applicant notes with appreciation the opportunity to discuss the subject application with the Examiner on April 30, 2003. A copy of the Interview Summary issued by the Examiner is attached hereto as Exhibit A.

Rejection Under 35 U.S.C. § 103(a)

The Examiner has rejected claims 1-6 and 8-24 of the present application under 35 U.S.C. § 103(a) over U.S. Patent No. 6,049,785 to Gifford (the "Gifford reference") in view of U.S. Patent No. 5,867,495 to Elliott et al. (the "Elliott reference").

In essence, the Examiner contends that the Gifford reference teaches:

> a processing system for processing a secure purchase order between a purchaser and a merchant across a public network comprising multiple data bases residing at the network payment system of which interconnects with both merchants and buyers or storing the account information for the purchase, a means for purchasing the purchase order and a purchaser identifier for identifying a particular purchaser.

The Examiner concedes, however, that the Gifford reference fails to disclose a disabler as set forth in the claims of the subject application. Nevertheless, the Examiner asserts that the Elliott reference teaches the claimed disabler and that it would have been obvious to one having ordinary skill in the art to have modified the teachings of Gifford to include the disabler of Elliott.

Applicant respectfully submits that independent claims 1, 14, 17, 20 and 22, as amended are allowable over Gifford in view of Elliott. The Gifford reference generally describes an open network payment system which permits authentication of payment orders based on a confirmation e-mail message. According to Gifford, in order to make a purchase, a Merchant is presented with a user's payment information either via a missing payment information document or via pre-authorized payment order. For example, as shown in FIG. 4 the user is presented with missing payment information document that is used to gather user account information for the requested purchase. In contrast to the subject application, the missing payment information

document requires the user to enter credit card account information into the form in order to effectuate the purchase. Further, as shown in connection with FIG. 10, in some instances, the merchant is already in possession of the user's credit card information. More specifically, in FIG. 10, message 47 includes the user's Visa account number. Thus, whether the user is entering credit card information on a website, or the merchant is already in possession of the user's account information, the purchasing system of Gifford fails to teach or suggest using the payment data to pay for the purchased goods or services "without exposing the payment data to the merchant", as set forth in the claims of the subject application. Thus, Gifford teaches away from the present application in that it teaches placing merchants in possession with the user's account information to effectual the payment of the items being purchased.

In stark contrast to Gifford, the subject application, as set forth by independent claims 1, 11, 14, 17, and 20, payment for goods and services is effected through a intermediate processing system for processing a secure purchase order between the purchaser and the merchant.

Furthermore, as per the Examiner's suggestion, Applicant has amended independent claims 1, 11, 14, 17, 20 and 22 to more clearly point out that the purchaser identifier is different from the payment data. Thus, in response to receipt of a purchase order including the purchaser identifier, which is some alpha numeric code that is different from the payment data (e.g., a credit or debit card account number), the processor retrieves the payment data and the delivery data from the purchaser account database, transmits the delivery data to the merchant to fulfill the purchase order, and uses the payment data to pay for the purchased goods or services without exposing the payment data to the merchant. Thus, according to the claims of the present application, as amended, the credit card account information, for example, or other information that will be used to pay for the goods or services being purchased, is never exposed to Merchants by the intermediary processing system, and therefore is not subject to being intercepted by potential hackers or thieves.

Moreover, by transmitting only delivery data, which includes at least one prestored delivery address for the purchaser, a purchaser receiving goods or services fraudulently purchased will know virtually immediately upon delivery of the goods or services that a fraudulent transaction has taken place. The Gifford reference does not disclose this feature.

Applicant respectfully submits that the hypothetical combination proposed by the Examiner of Gifford and Elliott is also improper. Unlike the Gifford reference, Elliott describes a billing scheme for a communications network, such as a telephone system. As such, the Elliott reference is in an entirely different field of endeavor as compared to Gifford and, therefore, is not properly combined with the Gifford reference pursuant to MPEP § 2141.01(a).

Furthermore, there is no teaching or suggestion in Gifford that the system should in any way be modified to include a disabler that disables the ability to make purchases using the purchaser identifier "in response to a monitor change in the delivery data associated with a particular purchaser identifier," as set forth in the claims. Thus, if a potential thief or even the purchaser him or herself attempt to change the prestored delivery data, the disabler of the present application disables the associated purchaser identifier such that no purchases can be made using that purchaser identifier. Gifford does neither teaches nor suggest this feature.

In addition, the "disabler" of Elliott is entirely different from the disabler of the claims of the subject application. The disabler of Elliott pertains to a boot-time routine that marks certain files as "non-executable". This routine is run to prevent an intruder from gaining access to certain programs and to prevent the delivery of Trojan horse viruses. The disabler of Elliott thus, functions in an entirely different manner from the disabler of the subject application, which, as stated above functions to deactivate a purchaser identifier in the event of a change to the delivery data. Elliott, therefore, fails to teach or disclose the disabler of the subject application.

Conclusion

Applicant has made a diligent effort to place the Application in condition for allowance and respectfully submit that claims 1-6 and 8-24 in light of the amendments and arguments set forth above are in condition for immediate allowance. Consequently, if the Examiner cannot issue immediate Notice of Allowance, the Examiner is respectfully requested to contact the undersigned attorney to discuss the outstanding issues.

Because this response is being timely filed, Applicant submits that no fees are due. Nevertheless, Applicant authorizes the U.S. Patent Office to charge any new and additional fees or charges, including for extensions of time, to Deposit Account No. 19-4709, if necessary.

Respectfully submitted,

REG. NO. 48,874

for Steven B. Pokotilow
Registration No. 26,405
Attorney for Applicant
Stroock & Stroock & Lavan LLP
180 Maiden Lane
New York, New York 10038
(212) 806-5400

VERSION WITH MARKINGS TO SHOW CHANGES

1. (Amended) A processing system for processing a secure purchase order between a purchaser and a merchant across a public network, the processing system comprising:

a purchaser account database for storing therein purchaser account information for each purchaser, the purchaser account information including at least a purchaser identifier for identifying a particular purchaser, payment data for effecting payment of purchased goods or services, and delivery data associated with said purchaser identifier, said delivery data including at least one delivery address of said purchaser for fulfillment of the purchase order;

a disabler for monitoring the status of the purchaser account information;

a processor for receiving the purchase order from said public network, said purchase order including said purchaser identifier;

wherein the purchaser identifier is any alpha-numeric code that is different from the payment data;

wherein, in response to receipt of the purchase order including the purchaser identifier, the processor retrieves the payment data and the delivery data from the purchaser account database corresponding to the purchaser identifier, transmits the delivery data to the merchant to fulfill the purchase order, and uses the payment data to pay for the purchased goods or services without exposing the payment data to the merchant; and

wherein, in response to a monitored change in the delivery data associated with a particular purchaser identifier, the disabler disables the purchaser identifier such that no purchases can be made using that purchaser identifier.

14. (Amended) A transaction processing service for facilitating the processing of a secure purchase order between a purchaser and a merchant across a public network, the processing service comprising:

a processing system, including:

a purchaser account database for storing therein purchaser account information for each purchaser, the purchaser account information including at least a purchaser identifier for identifying a particular purchaser, payment data for effectuating payment of the

purchase order, and delivery data associated with said purchaser identifier and containing a delivery address of said purchaser for fulfillment of the purchase order;

a disabler for monitoring the status of the purchaser account database and disabling the purchaser identifier in response to a monitored change in the purchaser account information; and

a processor for receiving the purchase order from said public network, said purchase order including said purchaser identifier;

wherein the purchaser identifier is any alpha-numeric code that is different from the payment data;

wherein the processor retrieves the delivery data and payment data associated with the purchaser identifier from the purchaser account database and transmits said delivery data associated with the purchaser identifier to be communicated to said merchant and effectuates payment for the purchase order without exposing the payment data to the merchant.

17. (Amended) A method of facilitating secure transactions between purchasers and merchants across a public network, comprising the steps of:

storing purchaser account information which includes at least payment data for paying for purchased goods and delivery data for delivery of the purchased goods to the purchaser;

issuing a purchaser identifier to a purchaser for use in purchasing goods from a merchant;

disabling the purchaser identifier in response to any change in the purchaser account information or if the purchaser account information is accessed by an unauthorized user;

receiving a purchase order to purchase a product wherein the purchase order includes the purchaser identifier;

retrieving the delivery data and payment data associated with the received purchaser identifier;

wherein the purchaser identifier is any alpha-numeric code that is different from the payment data;

effectuating payment for the purchased product using the payment data without exposing the payment data to the merchant; and

communicating only the delivery data for the purchaser identified by the purchaser identifier to the merchant.

20. (Twice Amended) A method of facilitating secure transactions between purchasers and merchants across a public network, comprising the steps of:

at a purchaser system having access to a merchant store system:

selecting a product offered for sale by the merchant, the product being associated with a product identifier;

transmitting a purchaser identifier from the purchaser system to the merchant store system;

at the merchant store system:

receiving the purchaser identifier;

generating a purchase order for the selected product that includes the purchaser identifier; and

communicating the purchase order to the processing system; and

at the processing system:

processing the purchase order to retrieve delivery data and payment data associated with the purchaser identifier;

<u>wherein the purchaser identifier is any alpha-numeric code that is different from the payment data;</u>

effectuating payment for the selected product without exposing the payment data to the merchant; and

communicating the delivery data corresponding to the purchaser identifier to the merchant.

22. (Amended) A purchasing system for facilitating secure electronic transactions between a consumer and a merchant, wherein a secure consumer account is stored on the purchasing system and the account includes consumer payment information and at least one delivery address for delivering purchased items; the purchasing system comprising:

a communication connection to a merchant system via a network;

a server system operative with programming to:

receive a request for payment from the merchant system in response to an order placed by the consumer with the merchant to purchase items, wherein the request for payment includes a unique consumer identifier unrelated to the consumer payment information which is associated with the secure consumer account;

retrieve the consumer payment information from the consumer account associated with the unique consumer identifier and effectuate payment for the order to the merchant;

retrieve the delivery address from the consumer account associated with the unique consumer identifier and transmit the delivery address to the merchant computer for delivery of the purchased item; and

wherein once the secure consumer account is established by the consumer and the unique consumer identifier is assigned to the consumer account, the at least one delivery address associated with the unique consumer identifier cannot be changed without causing the unique consumer identifier to be disabled.